

The invention claimed is:

1. 1. A method comprising:
  2. sending a control packet from a first endpoint of a tunnel through the
  3. tunnel to a second endpoint of the tunnel; and
  4. waiting at the first endpoint for a responsive control packet through the
  5. tunnel from the second endpoint before sending packets other than a control
  6. packet through the tunnel.
1. 2. The method of claim 1 wherein the tunnel is a secure tunnel.
1. 3. The method of claim 2 wherein the tunnel uses the IPSec security
2. protocol suite.
  1. 4. The method of claim 3 wherein the tunnel uses ESP in tunnel mode.
  1. 5. The method of claim 1 wherein the tunnel traverses at least one
  2. network address translator (NAT).
  1. 6. The method of claim 5 wherein the first endpoint is a client and the
  2. second endpoint is a server.
  1. 7. The method of claim 5 wherein the NAT implements VPN Masquerade.
  1. 8. The method of claim 1 wherein the control packet is an ICMP echo
  2. request packet and the responsive control packet is an ICMP echo reply packet.
  1. 9. The method of claim 3 wherein the tunnel is defined by an epoch, the
  2. epoch comprising one security association (SA) in each direction, each SA
  3. having a negotiated limited lifetime and defining the use of the ESP protocol in
  4. tunnel mode with negotiated authentication and/or encryption keys and with a
  5. security parameters index (SPI) chosen by the SA's destination.
  1. 10. The method of claim 9 wherein before the end of tunnel's lifetime the
  2. endpoints establish a new tunnel between them.

1        11. The method of claim 10 wherein a designated endpoint has  
2 responsibility for establishing the new tunnel and ignores requests initiated by  
3 the other endpoint to establish a new tunnel.

1        12. The method of claim 1 wherein the second endpoint waits for a  
2 packet from the first endpoint through the tunnel before using the tunnel to send  
3 any packets.

1        13. The method of claim 1 wherein if the first endpoint does not receive  
2 any packets through the tunnel for a predetermined time interval then the first  
3 endpoint sends through the tunnel a control packet to the second endpoint.

1        14. The method of claim 13 wherein if the first endpoint sends through  
2 the tunnel to the second endpoint a predetermined maximum number of control  
3 packets without receiving any packets through the tunnel then the first endpoint  
4 establishes a new tunnel to the second endpoint.

1        15. The method of claim 10 wherein if an endpoint is unable to complete  
2 the establishment of a new tunnel before a predetermined time limit then that  
3 endpoint abandons establishment of that tunnel and starts establishing a new  
4 tunnel.

1        16. The method of claim 15 wherein if an endpoint successively fails to  
2 establish a new tunnel for more than a predetermined maximum number of times  
3 then that endpoint closes the connection currently being used to establish  
4 tunnels with the other endpoint and opens another such connection.

1        17. The method of claim 16 wherein the connection used to establish  
2 tunnels between the endpoints is an IKE session.

1        18. A computer readable media tangibly embodying a program of  
2 instructions executable by a computer to perform a method, the method  
3 comprising:

4            sending a control packet from a first endpoint of a tunnel through the  
5    tunnel to a second endpoint of the tunnel; and

6            waiting at the first endpoint for a responsive control packet through the  
7    tunnel from the second endpoint before sending packets other than a control  
8    packet through the tunnel.

1            19. The computer readable media of claim 18 where in the method the  
2    tunnel is a secure tunnel.

1            20. The computer readable media of claim 19 where in the method the  
2    tunnel uses the IPSec security protocol suite.

1            21. The computer readable media of claim 20 where in the method the  
2    tunnel uses ESP in tunnel mode.

1            22. The computer readable media of claim 18 where in the method the  
2    tunnel traverses at least one network address translator (NAT).

1            23. The computer readable media of claim 22 where in the method the  
2    first endpoint is a client and the second endpoint is a server.

1            24. The computer readable media of claim 22 where in the method the  
2    NAT implements VPN Masquerade.

1            25. The computer readable media of claim 18 where in the method the  
2    control packet is an ICMP echo request packet and the responsive control  
3    packet is an ICMP echo reply packet.

1            26. The computer readable media of claim 20 where in the method the  
2    tunnel is defined by an epoch, the epoch comprising one security association  
3    (SA) in each direction, each SA having a negotiated limited lifetime and defining  
4    the use of the ESP protocol in tunnel mode with negotiated authentication and/or  
5    encryption keys and with a security parameters index (SPI) chosen by the SA's  
6    destination.

1        27. The computer readable media of claim 26 where in the method before  
2 the end of tunnel's lifetime the endpoints establish a new tunnel between them.

1        28. The computer readable media of claim 27 where in the method a  
2 designated endpoint has responsibility for establishing the new tunnel and  
3 ignores requests initiated by the other endpoint to establish a new tunnel.

1        29. The computer readable media of claim 18 where in the method the  
2 second endpoint waits for a packet from the first endpoint through the tunnel  
3 before using the tunnel to send any packets.

1        30. The computer readable media of claim 18 where in the method if the  
2 first endpoint does not receive any packets through the tunnel for a  
3 predetermined time interval then the first endpoint sends through the tunnel a  
4 control packet to the second endpoint.

1        31. The computer readable media of claim 30 where in the method if the  
2 first endpoint sends through the tunnel to the second endpoint a predetermined  
3 maximum number of control packets without receiving any packets through the  
4 tunnel then the first endpoint establishes a new tunnel to the second endpoint.

1        32. The computer readable media of claim 27 where in the method if an  
2 endpoint is unable to complete the establishment of a new tunnel before a  
3 predetermined time limit then that endpoint abandons establishment of that  
4 tunnel and starts establishing a new tunnel.

1        33. The computer readable media of claim 32 where in the method if an  
2 endpoint successively fails to establish a new tunnel for more than a  
3 predetermined maximum number of times then that endpoint closes the  
4 connection currently being used to establish tunnels with the other endpoint and  
5 opens another such connection.

1        34. The computer readable media of claim 33 where in the method the  
2 connection used to establish tunnels between the endpoints is an IKE session.